The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:

12/11/2012

SUBJECT:

Vulnerability in DirectPlay Could Allow Remote Code Execution (MS12-082)

OVERVIEW:

A vulnerability has been discovered in the way Microsoft DirectPlay handles specially crafted content. DirectPlay is a network protocol that is shipped with Microsoft DirectX. This vulnerability could allow for remote code execution if an attacker can convince a user to open a specially crafted Office document. Successful exploitation of this vulnerability could result in the execution of arbitrary code with full administrative privileges resulting in full control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full system rights.

SYSTEMS AFFECTED:

- Windows XP
- Windows Server 2003
- Windows Vista
- Windows Server 2008
- Windows 7
- Windows 8
- Windows server 2012

RISK:

Government:

- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **High**

Home users:High

DESCRIPTION:

A vulnerability has been discovered in the way Microsoft DirectPlay handles specially crafted Office documents. Specifically, this issue affects versions 9, 10.1, and 11.0 of DirectX. This vulnerability could allow for remote code execution if an attacker can convince a user to open a specially crafted Office document.

Successful exploitation of any of these vulnerabilities could result in an attacker gaining the ability to install programs; view, change, or delete data; or create new accounts with full administrative rights.

RECOMMENDATIONS:

The following actions should be taken:

- Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Remind users not to open e-mail attachments from unknown users or suspicious e-mails from trusted sources.
- Remind users not to download or open files from un-trusted websites.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.

REFERENCES:

Microsoft:

http://technet.microsoft.com/en-us/security/bulletin/ms12-082

CVE:

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1537

Security Focus:

http://www.securityfocus.com/bid/56839